Lattice Attacks on the DGHV Homomorphic Encryption Scheme

Abderrahmane Nitaj[1⋆] and Tajjeeddine Rachidi[2]

[1] Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse Normandie, France
abderrahmane.nitaj@unicaen.fr
[2] School of Science and Engineering
Al Akhawayn University in Ifrane, Morocco
T.Rachidi@aui.ma

Abstract. In 2010, van Dijk, Gentry, Halevi, and Vaikuntanathan described the first fully homomorphic encryption over the integers, called DGHV. The scheme is based on a set of m public integers $c_i = pq_i + r_i$, $i = 1, \cdots, m$, where the integers p, q_i and r_i are secret. In this paper, we describe two lattice-based attacks on DGHV. The first attack is applicable when $r_1 = 0$ and the public integers c_i satisfy a linear equation $a_2c_2 + \ldots + a_mc_m = a_1q_1$ for suitably small integers a_i, $i = 2, \ldots, m$. The second attack works when the positive integers q_i satisfy a linear equation $a_1q_1 + \ldots + a_mq_m = 0$ for suitably small integers a_i, $i = 1, \ldots, m$. We further apply our methods for the DGHV recommended parameters as specified in the original work of van Dijk, Gentry, Halevi, and Vaikuntanathan.

KEYWORDS: Homomorphic Encryption, Cryptanalysis, Lattice reduction.

1 Introduction

In the last ten years, cloud computing has gained major importance and widespread. Yet, a very important concern of cloud computing remains the security and privacy of data. A useful solution to this concern is the use of fully homomorphic encryption (FHE) to encrypt data stored remotely. Indeed, a fully homomorphic encryption scheme supports the computation of arbitrary functions on encrypted data, possibly distributed across the cloud, without the need to resort to decryption. Unfortunately, not all encryption schemes are fully homomorphic. For example, RSA [20] is only multiplicatively homomorphic: given two ciphertexts $c_1 \equiv m_1^e \pmod N$ and $c_2 \equiv m_2^e \pmod N$, one can compute the encrypted form of m_1m_2, that is $(m_1m_2)^e \pmod N$, without having to recover the plaintexts m_1 and m_2, simply by applying $c_1c_2 \equiv m_1^em_2^e \equiv (m_1m_2)^e \pmod N$. Similarly, ElGamal [7] is multiplicatively homomorphic. By contrast, Paillier [19]

⋆ Partially supported by SIMPATIC (SIM and PAiring Theory for Information and Communications security).

is additively homomorphic: given two ciphertexts $c_1 = g^{m_1} r_1^N \pmod{N^2}$ and $c_2 = g^{m_2} r_2^N \pmod{N^2}$, one can perform $c_1 c_2 = g^{m_1+m_2}(r_1 r_2)^N \pmod{N^2}$, which gives $m_1 + m_2$ without having to resort to the decryption of the ciphertexts c_1 and c_2. Another example of an additively homomorphic scheme is the Goldwasser-Micali scheme [10].

In 2009, Gentry [8], presented the first construction of a FHE scheme. Gentry's scheme supports both addition and multiplication on ciphertexts and consists of three main steps. The first step constructs a *somewhat* homomorphic scheme, which is limited to evaluating low-degree polynomials over encrypted data. The second step slightly modifies the *somewhat* homomorphic scheme to make it bootstrappable, i.e., capable of evaluating its own decryption circuit (operations). The third step transforms the bootstrappable *somewhat* homomorphic encryption scheme into a fully homomorphic encryption through a recursive self-embedding. The security of Gentry's scheme has been determined to be based on the worst-case hardness of solving specific problems in an ideal lattice, namely the shortest independent vector problem (SIVP) over ideal lattices in the worst-case (see [9]).

A key disadvantage of Gentry's scheme, however, is its computational inefficiency. Therefore, much effort has been made by the research community to find alternative efficient FHE schemes. In 2010, van Dijk, Gentry, Halevi and Vaikuntanathan [6] presented DGHV, a computationally efficient FHE scheme over the integers. This scheme is based on a set of public integers, $c_i = pq_i + r_i$, $i = 1, \ldots, m$, where the parameters p, q_i and r_i are secrets with the following size constraints:

- p is a prime number.
- η is the bit-length of the secret key p.
- ρ is the bit-length of the secret noises r_i.
- γ is the bit-length of the public integers c_i.

In [6,16,5], the security of DGHV has been studied against several attacks, which served the purpose of improving its security by defining optimal bounds for its parameter bit size (η, ρ, and γ). As reported in [16], these attacks can be categorized according to their underling techniques:

- **Brute force search** [6,3]: When $c_1 = pq_1$, this technique consists in removing the noise, say r_2 from c_2 by trying all possibilities for $r_2 \in (-2^\rho, 2^\rho)$ and computing $\gcd(c_1, c_2 - r_2)$ which gives p with overwhelming probability.
- **Continued fractions** [6,16]: This consists on recovering q_i/q_j from c_i/c_j using continued fractions, which yields immediate calculation of $p = \lfloor c_i/q_i \rceil$.
- **Attacks on the Approximate-GCD assumption** [6,16]: The recovery of p through the recovery of r_i or q_i, $i = 1, \ldots, m$, using a combination of lattice reduction and other techniques. These attacks include Coppersmith's technique [4], the method for solving simultaneous diophantine equations [15] and the orthogonal lattice attacks [6,16] (See Section 3 for more on these attacks).

Yet, a more direct way to break the DGHV scheme when $r_1 = 0$ consists in finding p and q_1 by factoring $c_1 = pq_1$. To date, the most efficient known methods to factor c_1 are the Number Field Sieve (NFS) [2] and the Elliptic Curve Method (ECM) [14]. As shown in [16] (p. 82, Table 7.1), the DGHV factorization problem of c_1 is considered as untractable if $p > 2^{261}$ and $c_1 > 2^{2911}$.

1.1 Our Contribution

In this paper, we propose two new attacks on the DGHV scheme. The starting point of both attacks are the existance of two linear equations involving the public integers c_i for $i = 2, \ldots, m$ and the secret parameter q_1 on the one hand, and the secret parameters q_i, $i = 1, \ldots, m$ on the other.

In the first attack, we suppose that $c_1 = pq_1$ and that $c_i = pq_i + r_i$ with $r_i \neq 0$ for $i = 2, \ldots, m$. To avoid factoring attacks on c_1, we also suppose that q_1 is prime. If q_1 is not coprime with one of the integers c_i for $2 \leq i \leq m$, then $\gcd(c_1, c_i) = q_1$ which will reveal $p = \frac{c_1}{q_1}$. Hence, q_1 is coprime c_i for $i = 2, \ldots, m$. Therefore for any integers $a_2, \ldots, a_{m-1}$, the integer $a_m \equiv -(a_2c_2 + \ldots + a_{m-1}c_{m-1})(c_m)^{-1} \pmod{q_1}$ exists and satisfies the linear integer relation $a_2c_2 + \ldots + a_mc_m = a_1q_1$ for an integer a_1. We will leverage this relationship and show that one can find the DGHV parameters p, q_i and r_i in polynomial time if the coefficients a_i, $i = 1, \cdots, m$ are suitably small. The attack uses Coppersmith's method for solving multivariate linear modular equations, as presented by Herrmann and May in [12].

In the second attack, we suppose that $c_i = pq_i + r_i$ for $i = 1, \ldots, m$. Let $G = \gcd(q_1, \ldots, q_m)$. Then $\frac{q_{m-1}}{G}$ is coprime with one $\frac{q_i}{G}$, $i \neq m-1$. Assume that $\frac{q_{m-1}}{G}$ is coprime with $\frac{q_m}{G}$. Let $a_1, \ldots, a_{m-2}$ be arbitrary integers. Define

$$a_{m-1} \equiv -\left(a_1\frac{q_1}{G} + \ldots + a_{m-2}\frac{q_{m-2}}{G}\right)\left(\frac{q_{m-1}}{G}\right)^{-1} \pmod{\frac{q_m}{G}}.$$

Then there exists an integer a_m such that

$$a_1\frac{q_1}{G} + \ldots + a_{m-2}\frac{q_{m-2}}{G} + a_{m-1}\frac{q_{m-1}}{G} + a_m\frac{q_m}{G} = 0,$$

or equivalently $a_1q_1 + \ldots + a_mq_m = 0$. This shows that the integers $q_1, \ldots, q_m$ are linked by infinitely many linear integer relations. We exploit this relation, and show that if the coefficients a_i, $i = 1, \ldots, m$ are sufficiently small, then one can efficiently find all the DGHV parameters. Unlike the first attack, this attack is based solely on lattice reduction techniques, namely the LLL algorithm [15].

For both attacks, we carry out experiments to verify the validity and the effectiveness of our methods. We also define the new bounds for DGVH secret parameters that resist our attacks, effectively improving on previously proposed optimal bounds [6],[16].

1.2 Organization

The rest of this paper is organized as follows: In Section 2, we briefly review the preliminaries necessary for both our attacks. Section 3 is dedicated to leading

attacks on the DGHV scheme. In Section 4, we present our first lattice-based attack on DGHV, that is when $r_1 = 0$ and the numbers c_i satisfy a linear equation $a_2c_2 + \ldots + a_mc_m = a_1q_1$ for suitably small integers a_i, $i = 2, \ldots, m$. In section 5, we present our second lattice-based attack, which is applicable when the integers q_i satisfy a linear equation $a_1q_1 + \ldots + a_mq_m = 0$ for suitably small integers a_i. We then conclude the paper in Section 6.

2 Preliminaries

In this section, we review the DGHV scheme parameters and the Approximate-GCD assumption upon which its security is based. We also recall Coppersmith's method for solving linear diophantine equations, and review the lattice reduction technique used in our new attacks on the DGHV scheme.

2.1 The DGHV Scheme over the Integers

In 2010, van Dijk, Gentry, Halevi and Vaikuntanathan [6] proposed a fully homomorphic encryption scheme based on m public integers $c_i = pq_i + r_i$ where the secret parameters p, q_i, r_i are such that:

- For $i = 1, \ldots, m$, c_i is a public integer of bit-length γ.
- p is a private prime number of bit-length η.
- For $i = 1, \ldots, m$, q_i is a private integer of bit-length $\gamma - \eta$.
- For $i = 1, \ldots, m$, r_i is a private random integer with $|r_i| < 2^\rho$.

In [6], it is shown that the scheme is semantically secure under the Approximate-GCD assumption which states the following:

Definition 1 (Approximate-GCD assumption).
Let γ, η, ρ be positive integers. For any η-bit prime number p, given m many positive integers $c_i = pq_i + r_i$ with m many $(\gamma - \eta)$-bit integers q_i and m many integers r_i satisfying $|r_i| < 2^\rho$, it is hard to find p.

The hardness of the Approximate-GCD assumption has been studied by Howgrave-Graham [13], and used in the study of the security of the DHGV scheme in [6] and [16], leading to the establishment of typical integer sizes that guarantee high security levels of DHGV. Therein, the values $\rho \approx \sqrt{\eta}$, $\gamma = \eta^3 + \eta$ are considered secure (see [6]).

2.2 Lattice reduction

Here we present some basics on lattice reduction techniques. Let $b_1 \ldots, b_d$ be d linearly independent vectors of $\mathbb{R}^n$ with $d \leq n$. The lattice $\mathcal{L}$ spanned by $b_1 \ldots, b_d$ is the set of all integer linear combination $x_1b_1 + \ldots + x_db_d$ of $b_1 \ldots, b_d$ with $x_1, \ldots, x_d \in \mathbb{Z}$. The set of vectors $(b_1 \ldots, b_d)$ is called a basis of $\mathcal{L}$ and d is its dimension. If B is the matrix of $b_1 \ldots, b_d$ in the canonical basis of $\mathbb{R}^n$, then

the determinant of $\mathcal{L}$ is $\det(\mathcal{L}) = \sqrt{B^t B}$, and the Euclidean norm of a vector $v \in \mathcal{L}$ is defined using the scalar product $\|v\| = \sqrt{v \cdot v}$.

Of interest to many applications and algorithms is the shortest non-zero vector in a lattice. Finding the shortest non-zero vector is a computationally hard problem known as the *Shortest Vector Problem (SVP)* that guarantees the security of many cryptographic schemes. However, Minkowski's theorem, which dates back to 1889, guarantees the existence of short vectors, i.e., non-zero vectors whose length is not too large as in the following theorem.

Theorem 1 (Minkowski). *Let $\mathcal{L}$ be a lattice. Then there exists a non-zero vector $v \in \mathcal{L}$ such that*

$$\|v\| \leq \sqrt{\dim(\mathcal{L})}\det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})}}.$$

Given a lattice $\mathcal{L}$ and its original basis $b_1 \ldots, b_d$, lattice reduction consists in finding another basis, where a short non-zero vector is easily determined. This can be achieved through different algorithms, whose running time is usually at least exponential in the dimension of the lattice d. However, the LLL algorithm of Lenstra, Lenstra, and Lovsz [15] can find, in polynomial time, short non-zero vectors in a lattice with reasonable dimension.

Theorem 2 (LLL). *Let $\mathcal{L}$ be a lattice spanned by a basis $(u_1, \ldots, u_d)$, then the LLL algorithm produces a new basis $(b_1, \ldots, b_d)$ of L satisfying*

$$\|b_1\| \leq 2^{\frac{d-1}{4}}\det(\mathcal{L})^{\frac{1}{d}},$$

in polynomial time.

Thus, finding a reduced basis using LLL leads to finding reasonably short vectors in polynomial time.

2.3 Coppersmith's method for solving linear diophantine equations

The LLL algorithm has many applications in cryptography, including solving diophantine equations. Using the LLL algorithm, Coppersmith [4] derived a method for finding small roots of univariate modular equations and bivariate equations. This strategy is know as Coppersmith's technique and has been heuristically generalized for finding small roots of multivariate linear equations. The following result by Herrmann and May [12] gives a sufficient condition under which small roots of a modular linear equation can be found in polynomial time.

Theorem 3 (Herrmann-May). *Let N be a composite integer of unknown factorization with a divisor $p \geq N^\beta$. Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a linear polynomial in n variables. One can find in polynomial time all solutions $\left(x_1^{(0)}, \ldots, x_n^{(0)}\right)$ of the equation $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ with $\left|x_1^{(0)}\right| < N^{\lambda_1}, \ldots, \left|x_n^{(0)}\right| < N^{\lambda_n}$ if*

$$\sum_{i=1}^{n} \lambda_i < 1 - (1-\beta)^{\frac{n+1}{n}} - (n+1)\left(1 - \sqrt[n]{1-\beta}\right)(1-\beta).$$

3 Former attacks on the DGHV Scheme

We recall here the main existing attacks on the DGHV scheme. For more details, we refer to [6] and [16]. Assume that we have an instance of DGHV with $c_1 = pq_1$ and $c_i = pq_i + r_i$, $i = 2, \ldots, m$ where the parameters p, q_i and r_i are secret. The task is to recover p. We recall that p is a η-bit prime and $0 < r_i < 2^\rho$.

3.1 Brute force on the remainder

A simple way to recover p is to remove the noise, say from c_2, by finding r_2, and then compute $p = \gcd(c_1, c_2 - r_2)$. This can be achieved by trying all integers r_2 with $0 < |r_2| < 2^\rho$. The complexity of this attack is obviously $\mathcal{O}(2^\rho)$. However, applying the method of Chen and Nguyen [3], one can find p with complexity $\mathcal{O}\left(2^{\rho/2}\right)$. As a consequence, removing the noise to recover p does not work in practice when ρ is sufficiently large.

3.2 Continued fractions

Using $c_1 = pq_1$ and $c_2 = pq_2 + r_2$, and given that q_1 and q_2 are prime numbers, one gets

$$\left| \frac{c_2}{c_1} - \frac{q_2}{q_1} \right| = \frac{|r_2|}{c_1}.$$

To recover $\frac{q_2}{q_1}$ as a convergent of the continued fraction expansion of $\frac{c_2}{c_1}$, we need $\frac{|r_2|}{c_1} < \frac{1}{2q_1^2}$, that is $2q_1|r_2| < p$. This is not possible if q_1 is much larger than p as for the recommended values for the DGHV parameters where q_1 is η^3-bit size while p is η-bit size.

3.3 Simultaneous Diophantine approximation

In [15], it is shown that the LLL algorithm can find a solution for the simultaneous diophantine approximations. That is, given n rational numbers $\alpha_1, \cdots, \alpha_n$ and ε with $0 < \varepsilon < 1$, one can efficiently find integers $p_1, \ldots, p_n$, and q such that, for $i = 1, \ldots, n$,

$$|q\alpha_i - p_i| \leq \varepsilon, \quad \text{and} \quad 1 \leq q \leq 2^{\frac{n(n+1)}{4}} \varepsilon^{-n}.$$

This can be applied to the DHGV scheme. Using $c_1 = pq_1$ and $c_i = pq_i + r_i$, we get for $i = 2, \ldots, m$

$$\left| q_1 \frac{c_i}{c_1} - q_i \right| = \frac{|r_i|}{p} < 2^{\rho - \eta}.$$

This gives $m - 1$ simultaneous diophantine approximations which can be solved by applying the LLL algorithm [15] to reduce a basis of a lattice of dimension m. The LLL algorithm will succeed under the condition:

$$q_1 \leq 2^{\frac{(m-1)m}{4}} \cdot 2^{-(\rho-\eta)(m-1)} = 2^{\frac{(m-1)m}{4} + (\eta-\rho)(m-1)}.$$

Since $q_1 \approx 2^{\gamma-\eta}$, then $\gamma - \eta \leq \frac{m(m-1)}{4} + (\eta - \rho)(m-1)$, which can be achieved if

$$m > -2\eta + 2\rho + \frac{1}{2} + \frac{1}{2}\sqrt{16\eta^2 - 32\eta\rho + 16\rho^2 + 16\gamma - 8\eta - 8\rho + 1}.$$

For secure DHGV parameters, such as $\gamma = \eta^3 + \eta$, $\rho \approx \sqrt{\eta}$ with a sufficiently large η, this gives a large lower bound for m, and in this case lattice reduction will not recover the shortest vector. For example, for $\eta = 200$ we get $m > 5297$, which makes the lattice reduction totally inefficient according to the optimal complexity bound $\mathcal{O}\left(m^4 \log B\mathcal{M}(m\log(B))\right)$ where B is an upper bound of the Euclidean norms of the basis vectors and $\mathcal{M}(k)$ denotes the time required to multiply k-bit integers (see [18]).

3.4 Orthogonal lattice attack

Another attack on DGHV is the orthogonal lattice attack [6,16]. Let $c_1 = pq_1$ and $c_i = pq_i + r_i$, for $i = 2, \ldots, m$. Then there exist $m-1$ integers a_i, $i = 2, \ldots, m$ such that $a_2c_2 + \ldots + a_mc_m \equiv 0 \pmod{c_1}$. This can be rewritten as

$$p(a_2q_2 + \ldots + a_mq_m) + a_2r_2 + \ldots + a_mr_m \equiv 0 \pmod{pq_1}.$$

Hence $a_2r_2 + \ldots + a_mr_m \equiv 0 \pmod{p}$, and when the integers a_i, $i = 2, \ldots, m$, satisfy $|a_i| \leq \frac{2^{\eta-1-\rho}}{m-1}$, then

$$\begin{aligned} |a_2r_2 + \ldots + a_mr_m| &\leq |a_2||r_2| + \ldots + |a_m||r_m| \\ &\leq (m-1) \cdot \max_i |a_i| \cdot \max_i |r_i| \\ &\leq (m-1) \cdot \frac{2^{\eta-1-\rho}}{m-1} \cdot 2^{\rho} \\ &\leq 2^{\eta-1}. \end{aligned}$$

Since $p > 2^{\eta-1}$, then $|a_2r_2 + \ldots + a_mr_m| < p$, that is $a_2r_2 + \ldots + a_mr_m = 0$. Finding many such a_i's, leads to recovering p using $\gcd(c_1, a_2c_2 + \ldots + a_mc_m) = p$.

4 Our First Lattice-based Attack on DGHV

In this section, we present our first attack on the DGHV scheme. We exploit the existence of a linear relation between the $c_2, \ldots, c_m$ and the factor q_1 of c_1 in the form

$$a_2c_2 + \ldots + a_mc_m = a_1q_1,$$

where $a_1, \ldots, a_m$ are integers (see section 1.1). We derive a condition on the size of each $|a_i|$ under which the above equation can be solved leading to the cryptanalysis of the scheme. After presenting the attack, we will present a comparison with the orthogonal lattice attack [6], and show that our attack significantly increases the bound of the parameters a_i leading to more successful attacks.

4.1 The attack

Theorem 4. *Let $c_1 = pq_1$ and $c_i = pq_i + r_i$, $i = 2, \ldots, m$, be m positive integers with $2^{\eta-1} < p < 2^{\eta}$, $2^{\gamma-1} < c_i < 2^{\gamma}$ and $|r_i| < p$ for $i = 2, \ldots, m$. Let $a_1, \ldots, a_m$ be m integers satisfying $|a_i| < 2^{\alpha_i}$ for $i = 2, \ldots, m$ and $a_2c_2 + \ldots + a_mc_m = a_1q_1$. Define $\beta = \frac{\gamma-\eta-1}{\gamma}$. If*

$$\sum_{i=2}^{m} \alpha_i < \left(1 - (1-\beta)^{\frac{m}{m-1}} - m\left(1 - \sqrt[m-1]{1-\beta}\right)(1-\beta)\right)(\gamma - 1),$$

then, one can find p, $q_1, \ldots, q_m$, $r_2, \ldots, r_m$ in polynomial time.

Proof. Suppose that $c_1 = pq_1$ and $c_i = pq_i + r_i$ for $i = 2, \ldots, m$. Let $a_1, \ldots, a_m$ be m integers satisfying $a_2c_2 + \ldots + a_mc_m = a_1q_1$. Then

$$a_2c_2 + \ldots + a_mc_m \equiv 0 \pmod{q_1}, \tag{1}$$

where q_1 is an unknown divisor of c_1. Suppose that $2^{\eta-1} < p < 2^{\eta}$ and $2^{\gamma-1} < c_1 < 2^{\gamma}$. Then, since $q_1 = \frac{c_1}{p}$, we get

$$2^{\gamma-\eta-1} < q_1 < 2^{\gamma-\eta+1}.$$

Define $\beta = \frac{\gamma-\eta-1}{\gamma}$. Then

$$q_1 > 2^{\gamma-\eta-1} = 2^{\gamma\beta} > c_1^{\beta}.$$

Using Herrman-May's Theorem 3, we can solve the equation (1) if the unknown parameters a_i satisfy $|a_i| < c_1^{\lambda_i}$ for $i = 2, \ldots, m$ where

$$\sum_{i=2}^{m} \lambda_i < 1 - (1-\beta)^{\frac{m}{m-1}} - m\left(1 - \sqrt[m-1]{1-\beta}\right)(1-\beta). \tag{2}$$

For $i = 2, \ldots, m$, define $\alpha_i = (\gamma - 1)\lambda_i$. Then

$$c_1^{\lambda_i} > 2^{(\gamma-1)\lambda_i} = 2^{\alpha_i}.$$

Now, suppose that $|a_i| < 2^{\alpha_i}$ for $i = 2, \ldots, m$. Then $|a_i| < c_1^{\lambda_i}$ and plugging $\alpha_i = (\gamma - 1)\lambda_i$ in equation (2), one can find the parameters a_i, $i = 2, \ldots, m$ if

$$\sum_{i=2}^{m} \alpha_i < \left(1 - (1-\beta)^{\frac{m}{m-1}} - m\left(1 - \sqrt[m-1]{1-\beta}\right)(1-\beta)\right)(\gamma - 1).$$

Using the recovered values of the parameters a_i for $i = 2, \ldots, m$, we compute

$$q_1 = \gcd(c_1, a_2c_2 + \ldots + a_mc_m), \quad p = \frac{c_1}{q_1}.$$

Next, for $i = 2, \ldots, m$, we find $r_i \equiv c_i \pmod{p}$ and $q_i = \frac{c_i - r_i}{p}$. □

Let us summarize the whole method in Algorithm 1.

Algorithm 1 : The first attack

Input: A set of **public values** $c_1 = pq_1$, $c_i = pq_i + r_i$, $i = 2, \ldots, m$.

Output: The set of private parameters p, q_i, $i = 1, \ldots, m$ if the conditions of Theorem 4 are fulfilled.

Set $f(x_2, \ldots, x_m) = c_2x_2 + \ldots + c_mx_m$.
Apply Coppersmith's technique and Herrman-May's Theorem 3 to solve the polynomial equation $f(x_2, \ldots, x_m) \equiv 0 \pmod{q_1}$.
For each solution $(x_2, \ldots, x_m)$ **do**
  Compute $g = \gcd(c_1, x_2c_2 + \ldots + x_mc_m)$.
  If $g > 1$ **then**
    Set $q_1 = g$ and $p = \frac{c_1}{q_1}$.
    For $i = 2, \ldots, m$ **do**
      Compute $r_i \equiv c_i \pmod{p}$.
      Compute $q_i = \frac{c_i - r_i}{p}$.
    End for
    Output p, q_i, $i = 1, \ldots, m$, r_i, $i = 2, \ldots, m$.
    Halt
  End if
End for

4.2 Comparison with the orthogonal lattice attack

Let us now compare our method with the orthogonal lattice attack of [6]. Suppose that $c_1 = pq_1$ and $c_i = pq_i + r_i$ for $i = 2, \ldots, m$. Let $a_2, \ldots, a_m$ be $m-1$ integers satisfying $a_2c_2 + \ldots + a_mc_m \equiv 0 \pmod{c_1}$ and $|a_i| < 2^\alpha$ as required in the orthogonal attack. Then, since $c_1 = pq_1$, we get $a_2c_2 + \ldots + a_mc_m \equiv 0 \pmod{q_1}$ which means that the equation can be exploited in our attack. Using Theorem 4, our attack can recover all the parameters p, q_1, q_i, r_i for $i = 2, \ldots, m$ if

$$\alpha < \frac{1}{m-1}\left(1 - (1-\beta)^{\frac{m}{m-1}} - m\left(1 - \sqrt[m-1]{1-\beta}\right)(1-\beta)\right)(\gamma - 1), \qquad (3)$$

where $\beta = \frac{\gamma - \eta - 1}{\gamma}$. Recall that the orthogonal attack of [6], as explained in Section 3.4, will find p if

$$|a_i| \leq \frac{2^{\eta-1-\rho}}{m-1} = 2^{\eta-1-\rho-\log_2(m-1)},$$

for $i = 2, \ldots, m$. So, define the bound for the orthogonal lattice attack of [6]

$$\alpha_0 = \eta - 1 - \rho - \log_2(m-1),$$

and the bound for our attack

$$\alpha_{\text{new}} = \frac{1}{m-1}\left(1 - (1-\beta)^{\frac{m}{m-1}} - m\left(1 - \sqrt[m-1]{1-\beta}\right)(1-\beta)\right)(\gamma - 1).$$

Let us compare α_0 and α_{new} in the optimal situation where $\eta \geq 200$, $\gamma = \eta^3 + \eta$ and $\rho \approx \sqrt{\eta}$ as recommended by [6]. These parameter sizes are believed to resist

currently known attacks including factorization, diophantine and lattice-based attacks. In Table 1, we show the maximal values of α_0 for which the orthogonal attack of [6] works, and the maximal values of α_{new} for which our attack works. Clearly, our method *significantly* increases the bounds of the size of the unknown integers a_i, $i = 2, \ldots, a_m$ for which DGHV is vulnerable.

	$m=2$		$m=3$		$m=5$		$m=10$		$m=15$	
η	α_0	α_{new}	α_0	α_{new}	α_0	α_{new}	α_0	α_{new}	α_0	α_{new}
200	184.8	7.9×10^6	183.8	3.9×10^6	182.8	1.9×10^6	181.6	8.8×10^5	181	5.7×10^5
300	284.8	2.6×10^7	283.8	1.3×10^7	282.8	6.7×10^6	281.6	2.9×10^6	281	1.9×10^6
400	384.8	6.3×10^7	383.8	3.1×10^7	382.8	1.5×10^7	381.6	7.1×10^6	381	4.5×10^6
500	484.8	1.2×10^8	483.8	6.2×10^7	482.8	3.1×10^7	481.6	1.3×10^7	481	8.9×10^6

Table 1. Comparison of α_0 and α_{new} for certain values of η and m.

4.3 Deriving new parameter sizes

To avoid the new attack, it is sufficient to make the inequality (3) impossible or hard to occur. Since γ is large, this could be possible if

$$1 - (1-\beta)^{\frac{m}{m-1}} - m\left(1 - \sqrt[m-1]{1-\beta}\right)(1-\beta) \approx 0,$$

where $\beta = \frac{\gamma-\eta-1}{\gamma}$. Therefore, for $m > 1$, our attack will fail if $\beta \approx 0$, or equivalently $\gamma \approx \eta$. However, our attack is likely to be successful when $\beta \approx 1$ and the number m of public integers c_i, $i = 1, \ldots, m$ is not very large. In this situation, the inequality (3) reduces to $\alpha < \frac{\gamma-1}{m-1}$. Note that $\beta \approx 1$ implies that γ is much larger than η which is the case for the currently recommended parameters. Therefore, for the recommended parameters $\gamma = \eta^3 + \eta$ with large η, our attack will be successful as long as $\alpha < \frac{\gamma-1}{m-1}$.

4.4 Experimental Results

We implemented our attack and experimented it with 100 instances of DGHV. All the 100 attacks were successful. For efficiency reasons, we considered only instances of DGHV where the sizes of the parameters are small, typically $\eta \leq 60$ and $\gamma \leq 200$. The recommended DHGV parameters $\eta \geq 200$ and $\gamma = \eta^3 + \eta$ i.e., $\gamma \geq 8000200$ are not suitable for experimentation using an off-the-shelf computer.
The following example is presented as a concrete illustration of our attack.

Consider the following situation with $m = 4$ public integers:

$$c_1 = pq_1 = 1156817133965493437022079142422608376953505161246136 57,$$
$$c_2 = pq_2 + r_2 = 1082255576771938594517495181665609305640555199978819 78,$$
$$c_3 = pq_3 + r_3 = 8700862799358141819065316312073487592675708173224241 0,$$
$$c_4 = pq_4 + r_4 = 6390073507222036838345230484304785647684242346947333 3,$$

where, for $i = 2, 3, 4$, $c_i < 2^\gamma$ with $\gamma = 177$. According to Theorem 4, we can solve the linear equation $a_2c_2 + a_3c_3 + a_4c_4 = a_1q_1$ if the unknown parameters a_2, a_3 and a_3 are suitably small. Combining the method of Herrmann and May [12] for solving the equation $a_2c_2+a_3c_3+a_4c_4 \equiv 0 \pmod{q_1}$, and the LLL algorithm [15], we get at least two polynomials sharing the solutions a_2, a_3, a_4. Then applying Gröbner Basis computation for solving systems of polynomial equations, we get the solution

$$a_2 = 130722418993,\ a_3 = 16613347,\ a_4 = 27131339.$$

Using these values, we get

$$\begin{aligned} q_1 &= \gcd(c_1, a_2c_2 + a_3c_3 + a_4c_4) \\ &= 2939299645410290951093220439666796843647265081, \\ p &= \frac{c_1}{q_1} = 39356897. \end{aligned}$$

Using the value of p, we get

$$\begin{aligned} r_2 &\equiv c_2 \equiv 13835383 \pmod{p}, \\ r_3 &\equiv c_3 \equiv 37261850 \pmod{p}, \\ r_4 &\equiv c_4 \equiv 1283090 \pmod{p}. \end{aligned}$$

Finally, we get

$$q_2 = \frac{c_2 - r_2}{p} = 27498498592811790891885993493481188459561616 35,$$
$$q_3 = \frac{c_3 - r_3}{p} = 22107593490813419104319419064143922709851104 81,$$
$$q_4 = \frac{c_4 - r_4}{p} = 16236222858783904733000750756099459893101436 19.$$

The whole process, including Gröbner Basis computation, took less than one minute. Note that since $a_2c_2 + a_3c_3 + a_4c_4 \not\equiv 0 \pmod{p}$, the orthogonal attack of [6] and [16] is not applicable to this DGHV instance.

5 Our Second Lattice Attack on DGHV

In this section, we consider the situation where the DGHV public values are of the general form $c_i = pq_i + r_i$, $i = 1, \ldots, m$, and there exists a linear relation between the q_i's of the form $a_1q_1 + \ldots + a_mq_m = 0$. We show that it is possible to solve the equation and recover all the private parameters, when specific conditions on the size of the unknown coefficients a_i, $i = 1, \ldots, m$ are fulfilled.

5.1 The attack

Theorem 5. *Let $c_i = pq_i + r_i$, $i = 1, \ldots, m$, be m positive integers with $c_1 < \ldots < c_m$ and $|r_i| < 2^\rho$ for $i = 1, \ldots, m$. Let $a_1, \ldots, a_m$ be m integers satisfying $|a_i| < 2^\alpha$ for $i = 1, \ldots, m$ and $a_1q_1 + \ldots + a_mq_m = 0$. If*

$$\alpha < \frac{1}{m}\log_2(c_m) + \log_2\left(\frac{\sqrt{m}}{m+1}\right) - \rho,$$

then, one can find p, $q_1, \ldots, q_m$, $r_1, \ldots, r_m$ in polynomial time.

Proof. Let $c_i = pq_i + r_i$ for $i = 1, \ldots, m$ with $r_i \neq 0$. Then, there exist m integers a_i, $i = 1, \ldots m$ such that $a_1q_1 + \ldots + a_mq_m = 0$. Combining the values of c_i for $i = 1, \ldots, m$, we get:

$$a_1c_1 + \ldots + a_mc_m = a_1r_1 + \ldots + a_mr_m. \tag{4}$$

Consider the $m \times m$ lattice $\mathcal{L} \subset \mathbb{Z}^m$ defined by the rows of the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & c_1 \\ 0 & 1 & 0 & \ldots & 0 & c_2 \\ 0 & 0 & 1 & \ldots & 0 & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & c_{m-1} \\ 0 & 0 & 0 & \ldots & 0 & c_m \end{bmatrix}.$$

The dimension of $\mathcal{L}$ is $\dim(\mathcal{L}) = m$ and the determinant is $\det(\mathcal{L}) = c_m$. Let $v \in \mathcal{L}$ be a target vector generated from the vector $u = (a_1, \ldots, a_m) \in \mathbb{Z}^m$, that is,

$$v = uM = (a_1, \ldots, a_{m-1}, c_1a_1 + \ldots + c_ma_m). \tag{5}$$

Minkowski's Theorem 1 for $\mathcal{L}$ asserts that there exists short non-zero vectors of size at most $\sigma(\mathcal{L})$ where

$$\sigma(\mathcal{L}) = \sqrt{\dim(\mathcal{L})}\det(\mathcal{L})^{\frac{1}{\dim(\mathcal{L})}} = \sqrt{m}c_m^{\frac{1}{m}}. \tag{6}$$

For our target vector v to be among the shortest non-zero vectors of the lattice $\mathcal{L}$, the inequality $\sigma(\mathcal{L}) > \|v\|$ must hold. Assume further that for $i = 1, \ldots, m$, we have $|a_i| \leq 2^\alpha$ and $|r_i| \leq 2^\rho$. Using (5) with $a_1q_1 + \ldots + a_mq_m = 0$, we get

$$\begin{aligned} \|v\| &= \left(\sum_{i=1}^{m-1} a_i^2 + (c_1a_1 + \ldots + c_ma_m)^2\right)^{1/2} \\ &= \left(\sum_{i=1}^{m-1} a_i^2 + \left(\sum_{i=1}^{m} a_ir_i\right)^2\right)^{1/2} \\ &< \left(2^{2\alpha}(m-1) + \left(2^{\alpha+\rho}m\right)^2\right)^{1/2} \\ &< \left(2^{2(\alpha+\rho)}\,(m+1)^2\right)^{1/2} \\ &= (m+1)2^{\alpha+\rho}. \end{aligned}$$

Therefore, the inequality $\sigma(L) > \|v\|$ is fullfiled if $\sqrt{m}c_m^{\frac{1}{m}} > (m+1)2^{\alpha+\rho}$, from which we deduce the following condition on α.

$$\alpha < \frac{1}{m}\log_2(c_m) + \log_2\left(\frac{\sqrt{m}}{m+1}\right) - \rho. \tag{7}$$

If the condition (7) holds, then applying lattice reduction to $\mathcal{L}$ yields the vector $v = (a_1, \ldots, a_{m-1}, c_1a_1 + \ldots + c_ma_m)$ with $c_1a_1 + \ldots + c_ma_m = a_1r_1 + \ldots + a_mr_m$, as in (4). Combining the obtained values from the reduction, that is $a_1, \ldots, a_{m-1}$ and $c_1a_1 + \ldots + c_ma_m$, and the known public values c_i, $i = 1, \cdots, m$, one can calculate a_m as follows:

$$a_m = \frac{(c_1a_1 + \ldots + c_ma_m) - (c_1a_1 + \ldots + c_{m-1}a_{m-1})}{c_m}.$$

The next step in the attack is to solve the equation

$$a_1r_1 + \ldots + a_mr_m = c_1a_1 + \ldots + c_ma_m, \tag{8}$$

with the unknown parameters $r_1, \ldots, r_m$ with $|r_i| < 2^\rho$ for $i = 1, \ldots, m$. To do so, we consider the $(m+1) \times (m+1)$ lattice $\mathcal{L}' \subset \mathbb{Z}^{m+1}$ defined by the rows of the matrix

$$M' = \begin{bmatrix} 1\,0\,0\ldots 0 & Ca_1 \\ 0\,1\,0\ldots 0 & Ca_2 \\ 0\,0\,1\ldots 0 & Ca_3 \\ \vdots\,\vdots\,\vdots\,\ddots\,\vdots & \vdots \\ 0\,0\,0\ldots 1 & Ca_m \\ 0\,0\,0\ldots 0 & C(c_1a_1 + \ldots + c_ma_m) \end{bmatrix},$$

where C is a given parameter to be optimized later. The determinant of $\mathcal{L}'$ is $\det(\mathcal{L}') = C|c_1a_1 + \ldots + c_ma_m|$ and its dimension is $\dim(\mathcal{L}') = m+1$.
Let $v' \in \mathcal{L}'$ be a vector. Then there exists a vector $u' = (y_1, \ldots, y_{m+1}) \in \mathbb{Z}^{m+1}$ such that

$$v' = u'M' = (y_1, \ldots, y_m, C(a_1y_1 + \ldots + a_my_m) + C(c_1a_1 + \ldots + c_ma_m)y_{m+1}).$$

We set our target vector to be $v' = (r_1, \ldots, r_m, 0)$, therefore

$$\begin{aligned} &y_1 = r_1, \ldots, y_m = r_m, \\ &(a_1y_1 + \ldots + a_my_m) + (c_1a_1 + \ldots + c_ma_m)y_{m+1} = 0. \end{aligned}$$

In addition, we need $y_{m+1} = -1$ so that $a_1r_1 + \ldots + a_mr_m = c_1a_1 + \ldots + c_ma_m$ which provides a solution to equation (8). Now recall that Minkowski's Theorem 1 asserts that there exist short non-zero vectors in the lattice $\mathcal{L}'$ of size at most $\sigma(\mathcal{L}')$ where

$$\sigma(\mathcal{L}') = \sqrt{\dim(\mathcal{L}')}\det(\mathcal{L}')^{\frac{1}{\dim(\mathcal{L}')}} = \sqrt{m+1} \cdot C^{\frac{1}{m+1}} \cdot |c_1a_1 + \ldots + c_ma_m|^{\frac{1}{m+1}}.$$

Since $c_1a_1 + \ldots + c_ma_m = a_1r_1 + \ldots + a_mr_m$ with $|a_i| < 2^\alpha$ and $|r_i| < 2^\rho$, then,

$$\sigma(\mathcal{L}') < \sqrt{m+1} \cdot C^{\frac{1}{m+1}} \cdot \left(2^{\alpha+\rho}m\right)^{\frac{1}{m+1}}. \tag{9}$$

The norm of our target vector $v' = (r_1, \ldots, r_m, 0)$ with $|r_i| < 2^\rho$ for $i = 1, \ldots, m$, satisfies

$$\|v'\| = \left(\sum_{i=1}^{m} r_i^2\right)^{1/2} < 2^\rho\sqrt{m}.$$

Therefore, for our target vector v' to be among the short vectors, the inequality $\sigma(\mathcal{L}') > \|v'\|$ must be satisfied. For this, it is sufficient that ρ satisfies

$$\sqrt{m+1} \cdot C^{\frac{1}{m+1}} \cdot \left(2^{\alpha+\rho}m\right)^{\frac{1}{m+1}} > 2^\rho\sqrt{m}$$

which leads to the following condition on C

$$C > m^{\frac{m-1}{2}} \cdot (m+1)^{-\frac{m+1}{2}} \cdot 2^{m\rho-\alpha}. \tag{10}$$

So, under condition 10, applying lattice reduction to $\mathcal{L}'$ recovers a short non zero vector $v' = (r_1, \ldots, r_m, 0)$ which yields the r_i's. Next, using r_1 and r_2, we get $p = \gcd(c_1 - r_1, c_2 - r_2)$ and for $i = 1, \ldots, m$, we get $q_i = \frac{c_i - r_i}{p}$. This terminates the proof. □

We can summarize the whole method in Algorithm 2.

5.2 Application with the DGHV recommended parameters

Let us consider the recommended optimal parameters for a secure DGHV, as stated in [6], that is $\gamma = \eta^3 + \eta$, $\rho \approx \sqrt{\eta}$ and $\eta \geq 200$. Then, the condition of Theorem 5 becomes

$$\alpha < \frac{\eta^3 + \eta}{m} + \log_2\left(\frac{\sqrt{m}}{m+1}\right) - \sqrt{\eta}.$$

On the other hand, the condition on the constant C in (10) becomes

$$C > m^{\frac{m-1}{2}} \cdot (m+1)^{-\frac{m+1}{2}} \cdot 2^{m\sqrt{\eta}-\alpha}.$$

In Table 2, we present the upper bounds for α in terms of η and m under which our second method will solve the equation $a_1q_1 + \ldots + a_mq_m = 0$ and then find all the DGHV parameters. For all cases, we use $C = 1$, wich fullfils condition (10).

η	$m = 2$	$m = 3$	$m = 5$	$m = 10$	$m = 15$
200	4×10^6	2.6×10^6	1.6×10^6	8×10^5	5.3×10^5
300	1.3×10^7	9×10^6	5.4×10^6	2.7×10^6	1.8×10^6
400	3.2×10^7	2.1×10^7	1.2×10^7	6.4×10^6	4.2×10^6
500	6.2×10^7	4.1×10^7	2.5×10^7	1.5×10^7	8.3×10^6

Table 2. Optimal values for α for different values of η and m.

Algorithm 2 : The second attack

Input: A set of ciphertexts $c_i = pq_i + r_i$, $i = 1, \ldots, m$.

Output: The set of private parameters p, q_i, $i = 1, \ldots, m$ if the conditions of Theorem 5 are fulfilled.

1: Define the lattice $\mathcal{L}$ with the basis matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & c_1 \\ 0 & 1 & 0 & \ldots & 0 & c_2 \\ 0 & 0 & 1 & \ldots & 0 & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & c_{m-1} \\ 0 & 0 & 0 & \ldots & 0 & c_m \end{bmatrix}.$$

2: Apply the LLL algorithm to reduce the basis matrix.
3: **For** each row $(a_1, \ldots, a_{m-1}, R)$ of the reduced matrix **do**
4: Compute $a_m = \frac{R-(c_1a_1+\ldots+c_{m-1}a_{m-1})}{c_m}$.
5: Compute $\alpha = \max_i (\log_2(|a_i|))$.
6: Compute $\rho = \frac{1}{m}\log_2(c_m) + \log_2\left(\frac{\sqrt{m}}{m+1}\right) - \alpha$.
7: Let C be the integral part of $m^{\frac{m-1}{2}} \cdot (m+1)^{-\frac{m+1}{2}} \cdot 2^{m\rho-\alpha} + 1$.
8: Define the lattice $\mathcal{L}'$ with the basis matrix

$$M' = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & Ca_1 \\ 0 & 1 & 0 & \ldots & 0 & Ca_2 \\ 0 & 0 & 1 & \ldots & 0 & Ca_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & Ca_m \\ 0 & 0 & 0 & \ldots & 0 & C(c_1a_1 + \ldots + c_ma_m) \end{bmatrix}$$

9: Apply the LLL algorithm to reduce the basis matrix.
10: **For** each row $(r_1, \ldots, r_{m+1})$ of the reduced matrix **do**
11: **If** $r_{m+1} = 0$ **then**
12: Compute $p = \gcd(c_1 - r_1, c_2 - r_2)$.
13: **If** $p > 1$ **then**
14: **For** $i = 1, \ldots, m$ **do**
15: Compute $q_i = \frac{c_i - r_i}{p}$.
16: **End for**
17: **End if**
18: **End if**
19: Output p, q_i, $i = 1, \ldots, m$, r_i, $i = 1, \ldots, m$.
20: Halt
21: **End for**
22: **End for**

5.3 Experimental Results

For our second attack, we also experimented with 100 DHGV instances with various practical sizes of the parameters η, ρ, γ and m. When the conditions of Theorem 5 are satisfied, we always succeeded in finding the solutions of our equations and recovered the secret parameters. We illustrate the steps of our attack through the following detailed example.
Consider the following DHGV instance:

$$c_1 = pq_1 + r_1 = 56405845507494530020941008480572940286181689237258854,$$
$$c_2 = pq_2 + r_2 = 39904821464460948494700284192336525523357407545067668,$$
$$c_3 = pq_3 + r_3 = 56294991345433284900612805613249060787237279328022519,$$

with the bounds $c_i < 2^\gamma$, $i = 1, 2, 3$, with $\gamma = 176$. According to Theorem 5, one can solve the equation $a_1q_1 + a_2q_2 + a_3q_3 = 0$ if the unknown coefficients a_i, $i = 1, 2, 3$ satisfy $|a_i| < 2^\alpha$ with

$$\alpha + \rho < \frac{1}{3}\log_2(c_3) + \log_2\left(\frac{\sqrt{3}}{4}\right) \approx 57.459,$$

where ρ is the bit size of the noise r_i, $i = 1, 2, 3$. Let $\mathcal{L}$ be the lattice spanned by the rows of the matrix

$$\begin{pmatrix} 1 & 0 & c_1 \\ 0 & 1 & c_2 \\ 0 & 0 & c_3 \end{pmatrix}.$$

Applying the LLL algorithm [15] for reduction, yields a reduced basis, where the first vector is $(3991298341123, 3713241313153, 18196712614595893)$. From this, we deduce

$$a_1 = 3991298341123,$$
$$a_2 = 3713241313153,$$
$$a_3 = \frac{18196712614595893 - (a_1c_1 + a_2c_2)}{c_3} = -6631296680887.$$

In this example, we have $|a_i| < 2^\alpha$ for $i = 1, 2, 3$ with $\alpha = 43$. Next, the aim is to solve the equation

$$a_1r_1 + a_2r_2 + a_3r_3 = a_1c_1 + a_2c_2 + a_3c_3 = 18196712614595893,$$

with the unknown coefficients r_1, r_2, and r_3. Let C be a constant, and consider the lattice $\mathcal{L}'$ spanned by the rows of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & Ca_1 \\ 0 & 1 & 0 & Ca_2 \\ 0 & 0 & 1 & Ca_3 \\ 0 & 0 & 0 & C(a_1c_1 + a_2c_2 + a_3c_3) \end{pmatrix}.$$

Then, using $C = 1$ and applying the LLL algorithm, we get the following short vector $(-23593, -18617, -21881, 0)$. This leads to the values of

$$r_1 = 23593, \qquad r_2 = 18617, \qquad r_3 = 21881.$$

Hence, in this example, we have $|r_i| < 2^\rho$ for $i = 1, 2, 3$ with $\rho = 15$. We then deduce

$$\begin{aligned}
p &= \gcd(c_1 - r_1, c_2 - r_2) = 706549229, \\
q_1 &= \frac{c_1 - r_1}{p} = 79832859753208406686890615063671579331921809, \\
q_2 &= \frac{c_2 - r_2}{p} = 56478472874338029310481752988136833029305319, \\
q_3 &= \frac{c_3 - r_3}{p} = 79675964582268739409540570899482307392394422.
\end{aligned}$$

In this example, we have $p < 2^\eta$ with $\eta = 30$. We notice that the dimensions of the underlying lattices are small and that the computation took less than 30 seconds using an off-the-shelf computer. Also, we notice that the condition of Theorem 5 is satisfied since

$$\alpha + \rho \approx \frac{1}{m}\log_2(c_m) + \log_2\left(\frac{\sqrt{m}}{m+1}\right) \approx 58.$$

More importantly, this example shows that while our second attack was successful, the existing attacks of [6], as described in Section 3, fail to recover the parameter p: the continued fraction attack fails because we need $\frac{|r_2|}{c_1} < \frac{1}{2q_1^2}$, which is not the case in this example, the simultaneous diophantine approximation attack fails too, because the condition on m should be

$$m > -2\eta + 2\rho + \frac{1}{2} + \frac{1}{2}\sqrt{16\eta^2 - 32\eta\rho + 16\rho^2 + 16\gamma - 8\eta - 8\rho + 1} > 9,$$

while $m = 3$ in this example. Finally, the orthogonal attack can not work since none of the $r_i = 0$.

6 Conclusion

In this paper, we presented two new lattice-based attacks on the DHGV encryption scheme using Coppersmith's technique and the LLL algorithm for the first attack, and only the LLL algorithm for the second attack. The first attack is applicable when $c_1 = pq_1$ and the $m - 1$ public integers c_i, $i = 2, \ldots, m$ satisfy a linear equation $a_2c_2 + \ldots + a_mc_m = a_1q_1$ for suitably small integers a_i, $i = 2, \ldots, m$. The second attack works even with $c_1 = pq_1 + r_1$ when the integers q_i satisfy a linear equation $a_1q_1 + \ldots + a_mq_m = 0$ for suitably small integers a_i, $i = 1, \ldots, m$. We illustrated our attacks by providing experimental results and examples, and further computed the bounds for DGHV recommended parameters for which our attacks are applicable, thus effectively extending on previously proposed optimal parameter bounds for p, c_i and r_i, $i = 1, \ldots, m$.

References

1. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 (2), pp. 203–213, (1999)
2. Buhler, J.P., Lenstra, H.W., Pomerance, C.: The development of the number field sieve, Volume 1554 of Lecture Notes in Computer Science, Springer-Verlag, 1994, pp. 50–94 (1994)
3. Chen, Y., Nguyen, P.Q.: Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers. In Pointcheval and Johansson (Eds.), EUROCRYPT 2012 Proceedings, volume 7237 of Lecture Notes in Computer Science. Springer, 2012, pp. 502–519 (2012)
4. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)
5. Coron, J.S., Mandal, A., Naccache, D., Tibouchi, T.: Fully homomorphic encryption over the integers with shorter public keys. CRYPTO 2011, In Rogaway (Eds.), Proceedings, volume 6841 of Lecture Notes in Computer Science. Springer, 2011, pp. 487–504 (2011)
6. van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully homomorphic encryption over the integers. In H. Gilbert (Ed.), EUROCRYPT 2010, LNCS, vol. 6110, Springer, 2010, pp. 24–43 (2010)
7. El Gamal, T.: A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31, pp. 496–473 (1976)
8. Gentry, C.: A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University (2009) Available at http: `http://crypto.stanford.edu/craig/craig-thesis.pdf`.
9. Gentry, C.: Toward basing fully homomorphic encryption on worst-case hardness, Crypto 2010, LNCS 6223, pp. 116–137 (2010)
10. Goldwasser, S., Micali, S.: Probabilistic Encryption. Journal of Computer and System Sciences, Vol 28, Issue 2, pp. 270–299 (1984)
11. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1975)
12. Herrmann, M., May, A.: Solving linear equations modulo divisors: On factoring given any bits. In Advances in Cryptology-ASIACRYPT 2008. Springer, 2008, pp. 406–424 (2008)
13. Howgrave-Graham, N.: Approximate integer common divisors. In CaLC'01, volume 2146 of Lecture Notes in Computer Science, pp. 51–66. Springer, (2001)
14. Lenstra, H.W.: Factoring integers with elliptic curves, Annals of Mathematics, vol. 126, pp. 649–673 (1987)
15. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)
16. Lepoint, T.: Design and Implementation of Lattice-Based Cryptography, Ph.D. thesis (2014)
`https://www.cryptoexperts.com/tlepoint/thesis/lepoint-phd-thesis.pdf`.
17. May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. Ph.D. thesis, University of Paderborn (2003)
`http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/`
18. Nguyen, P.Q. and Stehlé, D.: An LLL algorithm with quadratic complexity. SIAM J. of Computing, 39(3):874–903 (2009).
19. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In J. Stern (Ed.), EUROCRYPT'99, LNCS, vol. 1592, Spring, 1999, pp. 223–238 (1999)

20. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)